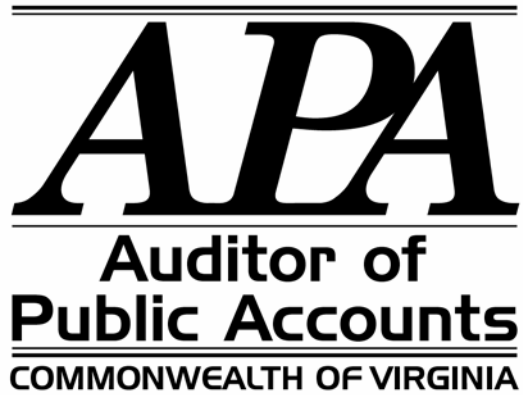
STATE CORPORATION COMMISSION

REPORT ON AUDIT

FOR THE YEAR ENDED

JUNE 30, 2005



AUDIT SUMMARY

Our audit of the State Corporation Commission, for the year ended June 30, 2005, found:

- proper recording and reporting of all transactions, in all material respects, in the Commonwealth Accounting and Reporting System and the Commission's accounting records;

- one matter involving internal control and the Commission's operations that requires management's attention and corrective action; and

- no instances of noncompliance with applicable laws and regulations, or other matters requiring reporting.

-TABLE OF CONTENTS-

AUDIT FINDING AND RECOMMENDATION

The State Corporation Commission (the Commission) does not have a complete or current information security program. The Commission's security program should include policies and procedures relating to all layers of information technology, including application, databases, and operating systems. Industry best practices provide that a well-developed security program should include documented policies and procedures covering the following basic areas.

- Business Impact Analysis
- Risk Assessment
- Business Recovery and Continuity Plan
- Information Security Management
- Information Systems Security Officer responsibilities

A comprehensive security program provides the necessary framework to protect the integrity of information systems and resources. Without a security program, the Commission does not know the current or potential risks to their systems; therefore, they cannot adequately prevent or minimize those risks.

Realizing the importance of having a security program, the Commission hired a vendor to perform a Security Policy and Operations Review. The review, completed in September 2005, assessed the Commission's state of security as benchmarked against industry-best practices. The Commission used the vendor's recommendations to create a corrective action plan and is currently ranking the recommendations based on risk, impact, and priority.

The Commission should allocate the time and resources necessary to complete a comprehensive information security program that will meet industry best practices and incorporate the vendor's recommendations before they are outdated.

AGENCY HIGHLIGHTS

The Commission is an independent agency directed by three commissioners, each elected by the General Assembly for six-year terms. Each commissioner administers specific divisions and the commissioners annually rotate the chairmanship.

The Commission has both regulatory and non-regulatory divisions. The regulatory divisions monitor such industries as utilities, state-chartered financial institutions, securities, retail franchising, insurance, and railroads. The Commission also serves as the Commonwealth's central filing office for corporations, limited partnerships, limited liability companies, business trusts, and Uniform Commercial Code filings. The non-regulatory divisions provide administrative and legal support. The Commission funds its operations from certain regulatory assessments and fees set by statue. The Commission also collects revenues for the General Fund, other special funds, localities and other state entities. The Commission collected a total of $463,419,495 in revenue for the General Fund in fiscal year 2005.

The regulatory and non-regulatory divisions are show below.

Regulatory Divisions:
- Insurance
- Securities and Retail Franchising
- Financial Institutions
- Public Service Taxation
- Public Utility Accounting
- Communications
- Energy Regulation
- Economics and Finance
- Utility and Railroad Safety
- Clerk of the Commission

Non-Regulatory Divisions:
- Commissioners' Offices
- General Counsel
- Hearing Examiners
- Commission Comptroller
- Information Resources
- Human Resources
- Information Technology

Regulatory Divisions

Bureau of Insurance

The Bureau of Insurance regulates over 1,400 insurance companies and 113,000 agents authorized to operate in Virginia. The Bureau examines the financial affairs of each domestic (Virginia-based) insurance company at least once every five years, and requires annual statements from foreign (based outside of Virginia) and alien (based outside of the United States) insurance companies doing business in Virginia. The Bureau also assists the public in resolving disputes with insurance companies.

The Bureau of Insurance collects revenue from a gross premium tax from insurance companies, which totaled $373,795,531 in General Fund revenue in fiscal year 2005. In addition, the Bureau collected $20.6 million in special revenue comprised of assessments and license, application, appointment, and other fees. The Bureau also collects an assessment from property and casualty insurance companies, which it transfers to the Department of Fire Programs, which in fiscal year 2005 was a transfer of $24.5 million.

The Bureau also collects special assessments for the Virginia Department of State Police to investigate insurance fraud. Each licensed insurer doing business in the Commonwealth, by writing any type of property and casualty insurance, except title insurance, pays a special assessment fee equal to a percentage of its direct gross premium income during the preceding calendar year. The Bureau can impose a late payment penalty of ten percent of the assessment and retains a portion of the special assessment to cover its

administrative expenses. The Bureau transferred $4.5 million in fiscal year 2005 to the Virginia Department of State Police.

The Bureau also receives uninsured motorist fees collected by the Department of Motor Vehicles (Motor Vehicles). In accordance with the Code of Virginia, the Bureau distributes these funds to the insurance companies who write automobile liability insurance. Motor Vehicles transferred uninsured motorist fees to the Bureau totaling $3.6 million in fiscal year 2005.

Division of Securities and Retail Franchising

The Division of Securities and Retail Franchising regulate security brokers and investment advisors in Virginia. The Division also registers franchises and trademarks in Virginia and investigates any reports of securities or franchising law violations or misconduct. The Division collected $8.17 million in special revenue during fiscal year 2005.

Bureau of Financial Institutions

The Bureau of Financial Institutions regulates and examines state-chartered banks, trust companies, savings and loans, and credit unions. The Bureau also licenses and examines mortgage lenders and brokers, and licenses and regulates money order sellers, consumer finance companies, industrial loan association's payday lenders, and credit counseling agencies. The Bureau collects revenue from these entities for application fees, license fees, annual assessment fees, examination fees, and investigation fees, which totaled $9.98 million in fiscal year 2005.

Division of Public Service Taxation

The Division of Public Service Taxation collects state taxes and fees on revenues and services of public service companies (e.g., electricity, water, and other power companies; telecommunications companies; and railroads). The Division collects taxes on electricity and natural gas based on a consumption tax imposed on the customers. The Division also determines and certifies the assessed value of utility company's property for local property taxation. In fiscal year 2005, the Division collected $83.2 million in General Fund revenue and $20.9 million in special revenue.

Division of Public Utility Accounting

The Division of Public Utility Accounting provides the Commission with accounting and financial information. The Commission uses this information when considering utility cases involving rates and services; affiliate transactions, mergers and acquisitions; certificates of public convenience and necessity; alternative regulatory plans; and the restructuring of utility markets.

Division of Communications

The Division of Communications regulates Virginia's telecommunications industry (other than the federally regulated cellular and wireless). This Division reviews rates and costs, evaluates telephone companies' performance, investigates consumer complaints regarding communications service, and oversees the implementation of telecommunications market competition.

Division of Energy Regulation

The Division of Energy Regulation regulates Virginia's investor-owned water and sewer, electric, and natural gas utilities, and member-owned electric cooperatives. This Division's responsibilities include reviewing rate applications filed by investor-owned utilities and member-owned cooperatives, monitoring utility construction projects, and responding to consumer complaints regarding electric, gas, and water and sewer utilities under the Commission's jurisdiction. The focus of electricity regulation is shifting from setting rates, to implementing the restructuring law under the guidance of the General Assembly.

Division of Economics and Finance

The Division of Economics and Finance advises the Commission on economic and finance issues related to public utilities, conducts research, and develops special studies and forecasts.

Division of Utility and Railroad Safety

The Division of Utility and Railroad Safety works to ensure safe operation of railroads within the Commonwealth by inspecting facilities, tracks, and equipment. To promote natural gas and hazardous liquid pipeline safety, the Division conducts pipeline facilities inspections, reviews records, and investigates incidents. The Division also investigates all reports of probable violations of the Underground Utility Damage Prevention Act. The Division provides free training relative to the Underground Utility Damage Prevention Act to stakeholders, conducts public education campaigns, and promotes partnership amongst various parties to further underground utility damage prevention in Virginia.

The Clerk of the Commission

The Clerk is the Commission's official custodian of judicial and administrative records. The Clerk's Office also serves as the central filing office for Uniform Commercial Code financing statements and federal tax liens as well as for thousands of corporations, partnerships, and limited liability companies doing business in Virginia. The Clerk's Office collects various fees from corporations, partnerships, and limited liability companies that register with the Commission. In fiscal year 2005, the Clerk's Office collected $6.46 million in General Fund revenue and $41.3 million in special revenue.

Non Regulatory Divisions

The non-regulatory divisions provide the Commission with administrative and legal support.

Financial Activity

The Department of Planning and Budget establishes an original budget based on the prior biennium budget amount, and adjusts for certain items. The following schedule compares the Commission's original and adjusted budgets with actual expenses.

Analysis of Budgeted and Actual Expenses

	2005		
Fund	Original Budget	Adjusted Budget	Actual Expenses
Special revenue	$78,698,495	$79,103,495	$66,510,803
Trust and agency	11,200,000	11,200,000	4,106,512
Federal	-	908,826	881,379
Total	$89,898,495	$91,212,321	$71,498,694

To determine their internal budget for non-personal expenses, the Commission uses prior year expenses and adjusts for one-time expenses. For personal services, the Commission bases their internal budget on 100 percent staffing levels. These methodologies account for the difference between the adjusted budget and the actual expenses for special revenue funds. The Commission's payroll expenses of $42,548,503 accounts for 59 percent of total expenses and contractual services accounts for 29 percent of total expenses.

In fiscal year 2005, Motor Vehicles transferred less uninsured motorist fees to the Commission for distribution to insurance companies. This uninsured motorist fees decrease is the cause for the variance between the adjusted budget and actual expenses for trust and agency funds.

The Commission funds its operations from certain regulatory assessments and fees set by statute, and records this activity primarily in four special revenue funds. Depending on the revenue source, the agency collects revenue annually, quarterly, or monthly. The Commission maintains a cash balance in these special revenue funds as a reserve to prevent a large fluctuation in rates. The Commission has determined that the reserve maintained should roughly equal expenses for six months. In 2000, in an effort to educate consumers relating to utility and telecommunications deregulation, the Commission increased the amount of the cash reserve to pay for the additional education expenses. Since this need has decreased, the Commission is making an effort to reduce cash balances by reducing fiscal year 2005 rates for certain activities. These efforts have reduced cash balances in special revenue funds by $4 million.

Commonwealth of Virginia

Walter J. Kucharski, Auditor

Auditor of Public Accounts
P.O. Box 1295
Richmond, Virginia 23218

June 7, 2006

The Honorable Timothy M. Kaine
Governor of Virginia
State Capital
Richmond, Virginia

The Honorable Thomas K. Norment, Jr.
Chairman, Joint Legislative Audit
and Review Commission
General Assembly Building
Richmond, Virginia

We have audited the financial records and operations of the **State Corporation Commission** for the year ended June 30, 2005. We conducted our audit in accordance with Government Auditing Standards, issued by the Comptroller General of the United States.

Audit Objectives

Our audit's primary objectives were to evaluate the accuracy of recorded financial transactions on the Commonwealth Accounting and Reporting System and in the Commission's accounting records, review the adequacy of the Commission's internal controls, test for compliance with applicable laws and regulations, and review corrective actions of audit findings from prior year reports.

Audit Scope and Methodology

The Commission's management has responsibility for establishing and maintaining internal control and complying with applicable laws and regulations. Internal control is a process designed to provide reasonable, but not absolute, assurance regarding the reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations.

We gained an understanding of the overall internal controls, both automated and manual, sufficient to plan the audit. We considered control risk in determining the nature and extent of our audit procedures. Our review encompassed controls over the following significant cycles, classes of transactions, and account balances.

Revenue
Contractual services expenses
Payroll expenses
Building maintenance
General controls over information systems

We performed audit tests to determine whether the Commission's controls were adequate, had been placed in operation, and were being followed. Our audit also included tests of compliance with provisions of applicable laws and regulations. Our audit procedures included inquiries of appropriate personnel and observation of the Commission's operations. We inspected documents including reconciliations, vouchers, contracts, timesheets, and monthly division revenue reports. We reviewed the applicable sections of the Code of Virginia and the 2005 Virginia Acts of Assembly. We tested transactions and performed analytical procedures, including budgetary and trend analyses.

Conclusions

We found that the Commission properly stated, in all material respects, the amounts recorded and reported in the Commonwealth Accounting and Reporting System, and in the Commission's accounting records. The Commission records its financial transactions on the cash basis of accounting, which is a comprehensive basis of accounting other than accounting principles generally accepted in the United States of America. The financial information presented in this report came directly from the Commonwealth Accounting and Reporting System.

We noted a matter involving internal control and its operation that require management's attention and corrective action. These matters are described in the section entitled "Audit Finding and Recommendation." However, the results of our tests of compliance with applicable laws and regulations disclosed no instances of noncompliance or other matters that are required to be reported under Government Auditing Standards.

The Agency has taken adequate corrective action with respect to audit findings reported in the prior year.

EXIT CONFERENCE AND REPORT DISTRIBUTION

We discussed this report with management on July 6, 2006. Management's response has been included at the end of this report.

This report is intended for the information and use of the Governor and General Assembly, management, and the citizens of the Commonwealth of Virginia and is a public record.

AUDITOR OF PUBLIC ACCOUNTS

TAS:sks
sks: 27

COMMONWEALTH OF VIRGINIA

JOEL H. PECK
CLERK OF THE COMMISSION
P. O. BOX 1197
RICHMOND, VIRGINIA 23218-1197

STATE CORPORATION COMMISSION

MEMORANDUM

DATE: July 10, 2006

TO: Walter J. Kucharski
Auditor of Public Accounts

FROM: Welton H. Jones, Jr.
Comptroller

Subsequent to discussing your Audit Finding and Recommendation with our Director of Information Technology the Commission agrees with the Recommendation. Please note the following additional information.

AUDIT FINDING AND RECOMMENDATION RESPONSE

Complete an Information Security Program

While our program is not complete the Commission does have an understanding of current or potential risks to its systems and a number of actions have been taken to remedy and prevent exposure. This has been accomplished through having a complete vulnerability and risk assessment done as a part of the Security Policy and Operations Review. The Security Program will be defined at a high level and in place within a year and the major activities associated with it will be complete or in progress. Of the items identified in the SCC Security Review report requiring attention and action, approximately 40 percent have been completed in line with industry best practices. Most of those remaining will be completed within the next twelve months but the larger ones may extend beyond that time and several will be ongoing by their nature.

Business Impact Analysis

As part of the Security Review, the business impact analysis created by the SCC as part of the Year 2000 remediation process was reviewed. It was found to still be essentially valid, but does require continuous appraisal and maintenance, which is an ongoing effort.

Risk Assessment

A risk assessment was completed as part of the Security Review. Many of the critical vulnerabilities and risks identified were immediately addressed and many of a lesser nature are being addressed. At the recommendation of the vendor, follow-up checks will be conducted internally approximately every 12 months using the software tools and methods from the Security Review to measure progress and to identify new risks or vulnerabilities.

Business Recovery and Continuity Plan

The Business Recovery and Continuity Plan needs to be significantly updated and strengthened to reflect current technology usage and requirements. This project will be started within the next 3-6 months, but its time frame for completion is unknown at this time. The availability of consulting expertise to assist in this activity is currently being researched with the process to procure this assistance to follow in an immediate time frame.

Information Security Management

Insofar as Information Security Management issues identified the following actions have been taken or are being addressed on both procedural and technical levels:

- Software Asset Management—ITD is in the procurement process for acquiring a software discovery tool to more effectively identify who has what software. The tool is called Express Software Manager. It can identify each desktop and the software running on it.
- Security Awareness—New employee security awareness training is conducted monthly. However, an ongoing program and training tools are being researched.
- Access Control— The SSID broadcast option for wireless access points was disabled. All wireless access points were upgraded from WEP to WPA encryption as recommended by the Unisys assessment. Industry best practices are being followed.
- Applications—SDLC and Business Requirements Analysis are being updated to include security as an analysis component. Several applications are being re-engineered with the .NET toolset. Oracle security patches were and are being applied as recommended.
- Firewall Solutions—A new PIX firewall solution was implemented in the Fall of 2005 with the following enhancements:

1. NTP configuration implemented
2. Access Control Statement changed to reflect the removal of the ip-any/any statement
3. ACS Server was configured and implemented to provide an additional level of authentication to firewall routers.

- Virtual Private Network Solution—SSH for remote management was implemented. Also IKE key exchange methods were adapted and the SCC does not permit user based VPN access.
- Wireless Networking—The SCC does not have a large wireless network but the 802.11i standards are being followed as previously documented in the Access Control bullet. WPA encryption is being utilized.
- Patch Management - For the infrastructure and desktops the SCC upgraded from Microsoft's SUS to WSUS patch management server. Updates are approved and done at least monthly. The SCC utilizes e-Trust as its virus management software.
- Data Base—upgrade to the current version of Listener was successfully implemented for Oracle 9i. DBAs are planning for the replacement of Oracle Forms with VB.NET and ASP.NET. Links between production/development/test servers were removed as recommended. Active User Lists were cleaned up and are reviewed quarterly. DB Scans are set up to run periodically and remove stored procedures.

Additionally, the SCC uses an outside vendor service to monitor for intrusions and to block SPAM.

Policies and Procedures

Procedures and standards related to the items above are being or will be developed as the items are addressed. An Information Technology Resource Usage policy is in place, and basic procedures for network and desktop security management exist. The Commission recognizes the need to be more aggressive in the area of developing policy, standards and procedures. Procedures and standards that have been implemented include: a Remote Access Standard, a Firewall/Router/Switch Security Standard and an IT Network Change management Procedure.

Information Systems Security Officer Responsibilities

The Information Systems Security Officer responsibilities are expanded significantly to encompass the areas identified in the review. However, current staff in this area (one analyst) is absorbed almost totally by the day-to-day

monitoring and support of current security functions. The review recognized this and indicated that additional professional staff would be required to develop further procedures and standards, to expand and complete implementation of the overall program and to oversee the program on an ongoing basis. A manager-level position has been identified in ITD's budget/plans and a request for creation of a position and recruitment is in process.

The SCC recognizes that it has not reached its goal of having a complete Information Security Program, but it has taken significant steps and is continuing to take steps to meet this objective. The SCC recognizes the critical importance of a security program and will further utilize the assessment report to pursue and attain this objective.

Cc: Mark C. Christie, Chairman
Theodore V. Morrison, Jr., Commissioner
Judith Williams Jagdmann, Commissioner

STATE CORPORATION COMMISSION

COMMISSION OFFICIALS

Clinton Miller, Chairman

Theodore V. Morrison Jr.

Mark C. Christie